

In the claims:

1. (currently amended) A system including at least two parts or stations wherein a transaction or connection between any two or more of said parts or stations is automatically conducted or established by means of an access code, said access code being available to an accessed part or station and requiring an identical access code to be provided to an accessing part or station at the time of conducting the transaction or establishing the connection, wherein said access code is one of a plurality of codes provided to said accessed part or station and available to said accessing part or station, said access codes being sent by means of an Internet download initiated by a software verification program resident in the system, from said accessed station into the accessing station, infinitely refreshed, said access code being selected from said plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code, preventing further use of a previously used code by means of said system being programmed to avoid re-using previously used codes for conducting further verifications, such that if an identical access code is not provided, the accessed part or stations requests three more access codes from the plurality of codes at the accessing part and requires an

212/656

identical match with a subsequent three access codes at the accessed part in order to conduct the transaction or establish the connection, ~~such that said previously used codes are not deleted but remain in an active state of service~~ wherein said verification failure renders said accessing station being denied permission to proceed with carrying out said transaction or connection; wherein said verification failure also renders said accessing station being barred from carrying out further electronic transactions or establishing further electronic connections; said system being programmed for sending verification messages to advise customers and subscribers of verification needs and security breaches.

2. (previously presented) A system according to claim 1 wherein said selected code is disabled after it has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations.

3. (currently amended) A system according to claim 1 wherein said plurality of codes is generated by means of a spreadsheet type program generator; and,

the system is programmed to mix a regular grid or pattern of characters or numbers in a controlled manner to produce non-repeating sequence of characters and numbers;

the system is programmed to disable previously used codes after they have been used for verification;

212/656

the system is programmed to select access codes for verification right at the time of the verification;

the system is programmed to avoid re-using previously used codes for verifications; such that, even if a similar replica or copy of a previously used code happens to be recycled or re-submitted for use; said software is programmed to avoid reusing them;

the system is programmed to selectively avoid using said disabled codes;

the system is programmed to prevent further use of a previously used code to avoid selecting such disabled previously used codes for verification, for establishing a secure connection or for conducting a secure transaction pseudo-random generator.

4. (previously presented) A system according to claim 1 wherein said plurality of codes is generated by means of a software program arranged to produce non-repeating sequence of codes.

5. (previously presented) A system according to claim 1 wherein each code includes a sequence of characters and numbers.

Claim 6 (cancelled).

7. (previously presented) A system according to claim 1 wherein the plurality of codes is generated external to said system.

8. (previously presented) A system according to claim 1 wherein said plurality of codes is at least 100.

212/656

9. (previously presented) A system according to claim 1 including first code storage means associated with said accessing part or station for storing one copy of said plurality of codes.

10. (previously presented) A system according to claim 9 including second code storage means associated with said accessed part or station for storing a second copy of said plurality of codes identical to said one copy stored in said first storage means.

11. (previously presented) A system according to claim 9 wherein said first code storage means includes one of an ATM transaction card, a smart card, an integrated circuit microchip and a computer diskette.

12. (previously presented) A system according to claim 10 wherein said second code storage means is associated with one of a bank computer system, a service provider computer system and a telephone exchange.

13. (previously presented) A system according to claim 1 wherein at least one said part or station includes an ATM terminal.

14. (previously presented) A system according to claim 1 wherein at least one said part or station includes a PC or computer terminal.

15. (previously presented) A system according to claim 1 wherein at least one said part or station includes a mobile transceiver.

212/656

16. (previously presented) A system according to claim 1 wherein at least one said part or station is associated with a door opening apparatus.

17. (currently amended) A method of automatically conducting a transaction or establishing a connection between at least two parts or stations by means of an access code, said access code being available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part or station, said method including the steps of:

making available a plurality of codes to said accessed and said accessing parts or stations;

said access codes being sent by means of an Internet download initiated by the verification software itself, from said accessed station into said accessing station;  
means of

selecting, at the time of conducting the transaction or establishing the connection, one code from said plurality of codes; means of

using said selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code;

preventing further use of a previously used code by means of said software being programmed to avoid re-using previously used codes for conducting future transactions or establishing future connections;

212/656

said access codes being present in storage means and memory devices selected from the group consisting of integrated circuit microchips, smart cards, magnetic strips, ATM cards and diskettes associated with the accessing part;

said accessing part being is selected from the group consisting of mobile transceivers, Automated Teller Machine terminals, personal computers and door opening apparatus;

wherein said system is operated to replenish said defunct storage means with fresh codes, upon being exhausted of valid access codes, through Internet downloads;

wherein said system is operated to replace said defunct or damaged storage means through personal selection and collection of storage means pre-loaded with new access codes from a service provider's branch office;

wherein said software is programmed to initiate a repeated verification sequence until it has achieved three consecutively successful verifications before access is granted;

wherein said verification failure renders said accessing station being denied permission to proceed with carrying out said transaction or connection; wherein,

said verification failure also renders said accessing station being barred from carrying out further electronic transactions or establishing further electronic connections; means wherein

212/656

said system being programmed for sending verification messages to advise users of verification status and security breaches.

~~said previously used codes are not deleted from said accessing and accessed parts and stations but remain in an active state of service;~~

~~infinitely rejuvenating and refreshing with new codes via auto-loading; and verifying said access codes by an interactive multiple strike challenge response mechanism.~~

18. (currently amended) A method according to claim 17 wherein said software verification module is programmed to avoid re-using said selected code for further verification ~~selected code is removed from said accessed part or station or is otherwise disabled~~ after it has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations.

19. (currently amended) A method according to claim 17 wherein the plurality of codes is generated by means of a ~~pseudo-random generator~~ spreadsheet type program generator; and

the system is programmed to mix a regular grid or pattern of characters or numbers in a controlled manner to produce non-repeating sequence of characters and numbers; means wherein;

the system is programmed to select access codes for verification right at the time of the verification;

selecting access codes for verification right at the time of the verification; means of

212/656

said system is programmed to avoid re-using previously used codes for verifications; such that, even if a similar replica or copy of a previously used code happens to be recycled or re-submitted for use; said software is programmed to avoid reusing them; means wherein

said system is programmed to selectively avoid using said disabled codes; means of,

said system is programmed to prevent further use of a previously used code by means of a verification software running on the computer programmed to avoid selecting such disabled previously used codes for verification, for establishing a secure connection or for conducting a secure transaction.

20. (previously presented) A method according to claim 17 wherein said plurality of codes is generated by means of a software program arranged to produce non-repeating sequence of codes.

21. (previously presented) A system according to claim 17 wherein each code includes a sequence of characters and numbers.

Claim 22 (cancelled).

23. (previously presented) A method according to claim 17 wherein the plurality of codes is generated external to said at least two parts or stations.

24. (previously presented) A method according to claim 17 wherein said plurality of codes is at least 100.



212/656

25. (previously presented) A method according to claim 17 including providing first code storage means associated with said accessing part or station for storing one copy of said plurality of codes.

26. (previously presented) A method according to claim 25 including providing second code storage means associated with said accessed part or station for storing a second copy of said plurality of codes identical to said one copy stored in said first storage means.

27. (previously presented) A method according to claim 25 wherein said first code storage means includes one of an ATM transaction card, a smart card, an integrated circuit microchip and a computer diskette.

28. (previously presented) A method according to claim 26 wherein said second code storage means is associated with one of a bank computer system, a service provider computer system and a telephone exchange.

29. (previously presented) A method according to claim 17 wherein at least one said part or station includes an ATM terminal.

30. (previously presented) A method according to claim 17 wherein at least one said part or station includes a PC or computer terminal.

31. (previously presented) A method according to claim 17 wherein at least one said part or station includes a mobile transceiver.

212/656

32. (previously presented) A method according to claim 17 wherein at least one said part or station is associated with a door opening apparatus.

Claims 33-34 (canceled)

35. (currently amended) A method of establishing a secure connection between a provider and a customer, comprising the steps of:

providing a smart card magnetic strip on a card for storing a first group of codes with the customer, said codes being sent to said customer by means of an Internet download;

providing a computer for storing a second group of codes with the provider, said second group of codes being identical to the first group of codes;

receiving a first code from the customer during establishing the secure connection, the first code being selected from the first group of codes by the verification software program; means of ~~without manual customer intervention~~

accessing a second code from the second group of codes;

comparing the first code with the second code, wherein a perfect match is a successful verification; and

preventing further use of said selected code by means of said verification software being programmed to avoid re-using previously used codes; means wherein,

212/656

upon being exhausted of valid access codes, said defunct storage means is self-replenished with fresh codes through Internet downloads;

sent directly from said service provider's verification computer system into said customer's electronic communications access device and smart card storage means;

said software being programmed to initiate a repetitive verification sequence until it has achieved three positive consecutive verifications to establish the identity of said customer; means wherein,

~~said verification failure rendering said customer being denied permission to proceed with carrying out said transaction or connection; wherein,~~

~~said verification failure renders said account being barred from carrying out further electronic transactions or establishing further electronic connections; means of~~

said software being programmed for sending verification messages to advise users of verification needs and security breaches. the first code by the customer by disabling the first code and the second code without manual customer intervention.

Claim 36 (cancelled).

37. (currently amended) A method as recited in claim 35, further comprising the steps of:

212/656

activating a code replacement module within the computer based upon a triggering event; wherein, said

triggering event being detection of a verification utilizing the 490<sup>th</sup> access codes (out of 500) stored in said storage means is disabling of a specified number of codes; means of,

automatically loading new codes into the smart card from onto the magnetic strip by the code replacement module 47 by means of an Internet download.

38. (previously presented) A method as recited in claim 35, wherein the automatic loading is an Internet download.

39. (previously presented) A method as recited in claim 35, wherein the automatic loading is conducted between wireless devices.

40. (currently amended) A method as recited in claim 35, further comprising the steps of:

performing verifications until all the codes are used up or spent;

providing a second smart card having been pre-loaded with a third group of access codes;

replacing said defunct storage means with said new smart card personally selected and collected from the service provider's branch office;

storing in the computer a fourth group set of codes identical to said third group ~~third set~~ of codes stored in said new smart card to allow continuing comparing

212/656

codes for the perfect match to allow the successful verification;

such that no two transactions are conducted or no two connections are established with a previously used code stored in the third and fourth group of codes; by means of a

verification software programmed to avoid re-using previously used codes for conducting future transactions or establishing future connections.

~~providing a second magnetic strip to the customer, the second magnetic strip having a third set of codes, replacing the magnetic strip on the card with the second magnetic strip; and~~

wherein the third and fourth set of codes never can have a code that has been used before

41. (currently amended) A computerized code based door opening apparatus for accessing a safe room or high security area comprising:

a user ~~portion that is~~ inaccessible part (accessed part) for controlling access to said safe room or high security area;

first storage means within the accessed part ~~portion~~ for storing a first group of codes;

second storage means in possession of the user for storing a second group of codes, wherein when the user requires access to the safe room, the second storage means serves

212/656

as an electronic key to gain access by providing an ~~unused~~ a valid code to the accessed part, said accessed part requiring an identical ~~unused~~ valid code from the first storage means to grant access to the safe room, wherein the groups of codes ~~may be~~ are automatically replenished based upon a triggering event such that each code is used only once.

42. (currently amended) A system according to claim 17 including means wherein said selected code is disabled ~~deactivated and decommissioned~~ after it selected code has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations; in order to prevent said previously used code from being re-used.

43. (previously presented) A system according to claim 17 further comprising the step of initially receiving a password to serve as a primary level of security between the accessed part and the accessing part.

44. (previously presented) A system as recited in claim 1, wherein a verification of access codes is conducted separately and independently of a password and PIN verification.

45. (previously presented) A system as recited in claim 1, further comprising software means for generating the access codes within a spreadsheet program, wherein, a pattern of character and numbers are manually mixed in a manipulated combination process to generate access codes.

46. (previously presented) A system as recited in claim 45, wherein the software means is externally located to the accessing and accessed parts.

212/656

47. (previously presented) A system as recited in claim 45, wherein upon completion of download or transfer of additional aaccess codes from said software means a self-destruct mechanism is automatically activated by the software means to permanently remove and delete all traces of said access codes.

48. (currently amended) A method as recited in claim 45, including means wherein the access codes are replenished ~~refreshed~~ in groups; wherein each group contains 500 pieces of access codes.

49. (currently amended) A fully automatic method of establishing a secure connection between a provider and a customer, comprising the steps of:

providing an active memory-storage means present on a card for storing a first group of codes associated with a customer's electronic utility appliance, wherein

said active memory-storage means comprises ~~being smart~~ cards and integrated circuit microchips;

said appliances being selected from the group consisting of mobile transceivers, ATM terminals, personal computer and door opening apparatus;

providing a computer for storing a second group batch of codes with the provider, said second group batch of codes being identical to the first group of codes; means of

providing a ~~software program~~ verification software program running on said computer for automatically selecting, requesting (challenge), and receiving a first code sent (response) from the customer during establishing a secure

212/656

connection, the requested selected first code being chosen from amongst the first group of codes without manual customer intervention; means of,

accessing a second code from the second group of codes in a similar manner;

comparing the first code with the second code, wherein a perfect match is a successful verification; and

preventing further use of said used ~~a verified~~ code by the customer by means of using a verification software program running on the computer ~~to~~ automatically programmed to recognize avoid reusing such previously used codes; means wherein, ~~spent them, wherein previously used codes are not deleted but continues to remain in an active state of service.~~

upon failure of an initial verification, said software is automatically programmed to initiate a repetitive verification sequence until it has achieved three positive consecutive verifications in order to establish the identity of said customer or subscriber; means wherein

~~said verification failure renders said customer being denied permission to proceed with carrying out said transaction or connection; means wherein,~~

~~said verification failure also renders said account being barred from carrying out further electronic transactions or establishing further electronic connections; means of~~



212/656

said software being automatically programmed for sending verification messages to advise customers and subscribers of verification needs and security breaches.

50. (currently amended) A method as recited in claim 49, wherein said integrated circuit microchips, are ~~may be~~ used as independent, stand-alone memory devices directly used and associated with said user's electronic utility appliances.

51. (currently amended) A method as recited in claim 49, wherein said memory-storage means comprises ~~may be~~ smart cards.

52. (currently amended) A method as recited in Claim 50, further comprising the steps of:

initiating a trigger mechanism to verify said access codes, said trigger mechanism being a positive verification by PINs and passwords;

using three way transmission traffic during the verification process;

using a "real time" interactive "challenge-response" mechanism wherein, verifications are carried out at the point in time of a connection being made, or transaction being conducted;

using an auto-selection mechanism for selecting specific access codes for verification, wherein usage of the codes is managed by a verification software program programmed to disable previously used codes in order to avoid reusing them.

212/656

53. (previously presented) A method as recited in claim 52,  
further comprising of the steps of:

using a fully automated variable access codes verification  
process without the user's interference or manual work.

54-67. (cancelled).